

Abstract

Vulnerabilities of complex networks have become a trend topic in complex systems recently due to its real world applications. Most real networks tend to be very fragile to high betweenness adaptive attacks. However, recent contributions have shown the importance of interconnected nodes in the integrity of networks and module-based attacks have appeared promising when compared to traditional malicious non-adaptive attacks. In the present work we deeply explore the trade-off associated with attack procedures, introducing a generalized robustness measure and presenting an attack performance index that takes into account both robustness of the network against the attack and the run-time needed to obtain the list of targeted nodes for the attack. Besides, we introduce the concept of deactivation point aimed to mark the point at which the network stops to function properly. We then show empirically that non-adaptive module-based attacks perform better than high degree and betweenness adaptive attacks in networks with well defined community structures and consequent high modularity.

Performance of attack strategies on modular networks

Bruno Requião da Cunha

*Polícia Federal, Brazil
Instituto de Física, Universidade Federal do Rio Grande do Sul,
Porto Alegre, RS, Brazil*

Sebastián Gonçalves

*Instituto de Física, Universidade Federal do Rio Grande do Sul,
Porto Alegre, RS, Brazil*

August 10, 2016

1 Introduction

Structural vulnerabilities of real systems have attracted much attention from the network science community recently [1, 2] both from the attack point of view (when we are interested in disabling or fragmenting a network with as little effort as possible) [3] and from the security point of view (when we wish to create safer networks or to defend them against targeted or malicious attacks) [4]. For instance, the operation of internet routers [5], the delivery of drugs in biological systems, the propagation of an epidemic disease [6], the security of a power grid [7, 8], or even the operativeness of organized crime or terrorist cells [9] are all examples of networking systems in which we are much interested either in devising efficient attack strategies to rapidly atomize the network [10] or in adopting defensive actions to prevent the system from collapsing [11].

Networks might be structurally affected either by random removal of nodes (failures) or by targeted or malicious attacks [12–15]. Targeted attacks are usually aimed to disrupt the system by removing a small fraction of nodes or edges. In this sense, traditional attack methods usually focus on the sorting of nodes according to their importance in the network architecture, *i.e.* according to some centrality index —betweenness and degree-based attacks usually present better results [16].

Basically there are two approaches for network fragmentation: non-adaptive (or simultaneous) attacks and adaptive (or sequential) attacks. In the first

approach, the list of attacked nodes or edges is produced only once, before the removal procedure starts [16]. In the second [17, 18] approach, the list of targets is updated after each deletion by recalculation of the centrality index used to sort nodes or edges. Consequently, high adaptive attacks demand more processing time, but on the other hand the method usually produces more damage per removal when compared to the non-adaptive approach. The reason is more or less obvious: if the list of attack is measured only once, the method cannot account for the changes in the centrality order due to the removal of elements. So, in the worst case the high adaptive version of a procedure is as good as the non-adaptive approach, however it is generally better.

Nonetheless, real networks tend to organize into modular structures or communities —clusters densely connected internally but sparsely connected among them [19]— and recently it was shown that the nodes bridging communities are even more crucial in keeping networks from falling apart than highly connected vertices [20, 21]. Even more recently, it was shown empirically that module-based attacks (MBA) targeting interconnected nodes (communities bridge) can damage real networks with more efficiency than other non-adaptive targeted attacks [22].

Hereupon, although there has been much work recently on network robustness, the balance between a given network damage and the computational cost (run time and/or hardware capacity) necessary to reach that desired level of fragmentation is an issue not yet properly addressed by previous contributions.

Usually the only aspect taken into account is the efficiency in terms of the ratio between the damage produced and the fraction of removed nodes. In this contribution, apart from that feature, we consider the trade-off between the network robustness and the computational cost of a given network attack strategy. More precisely, we focus on the cost/benefit relation of adaptive and non-adaptive attacks to modular networks in order to rightly chose the most appropriate strategy to atomize large complex networks.

2 Module-based attacks

The MBA procedure mentioned above is a non-adaptive attack which consists of targeting interconnected nodes ordered by betweenness centrality. Besides, once a node from a edge between two connected modules is deleted, there is no need to erase its counterpart unless it still connects to other communities —the vertices belonging to this set are called independent interconnected nodes. Furthermore, the attack is aimed at the largest remaining connected component of the network after each step. As detailed in [22] in module-based attacks for real networks, the communities are usually extracted by an heuristic community detection algorithm due to the size of such systems and consequent computational requirements. Besides, the effectiveness of the MBA procedure is closely related to the modularity of the network.

The modularity of an unweighted network is usually defined as the density of links inside communities as compared to links between communities, as

follows [1]:

$$Q = \frac{1}{2m} \sum_{i,j} \left[A_{ij} - \frac{k_i k_j}{2m} \right] \delta(c_i, c_j) \quad (1)$$

where A_{ij} is the adjacency matrix (taking the value 1 when there is a link between nodes i and j , 0 otherwise), k_i is the vertex degree of node i and c_i represents the community to which this node belongs. The δ -function $\delta(u, v)$ is 1 if $u = v$, 0 otherwise and m is the total number of edges.

In this sense, many methods for community detection have been devised over the last few years. Therefore, the issue of testing the accuracy of community extraction algorithms is crucial in studying modular networks. In order to test the performance of algorithms for community extraction (or identification), several benchmark for computer generated networks, with well-defined community, structures have been proposed. One of the first introduced benchmarks for testing community detection is a class of artificial undirected networks proposed by Girvan and Newman (GN) [23]. It consists of networks with nodes having approximately the same degree, as in a random graph, but with nodes preferentially connected to nodes of their group. However, real networks have heterogeneous distributions of node degree and community size accounting for several remarkable features of real networks, such as resilience to random failures/attacks and the absence of a threshold for percolation and epidemic spreading. In this sense Lancichinetti, Fortunato, and Radicchi have proposed an undirected network benchmark (LFR) [24] which assumes that both degree and community size distributions are power laws.

In these benchmarks, the modularity is controlled by the mixing parameter μ , which is the ratio between the number of edges linking a vertex to other communities and its degree. In other words, each node shares a fraction μ of its edges with nodes of the entire network and a fraction $1 - \mu$ of its edges with nodes of its own community. Thence, small values of μ indicate well separated module, whereas higher values means communities are ill defined and possibly overlapped. It should also be noted from now on that the average module size usually depends on the accuracy and the detection threshold of the community extraction algorithm. However, as pointed out in [25] the *Louvain* algorithm by Blondel *et al.* [26] is known to perform very precisely in both GN and LFR benchmarks. Therefore, in simulations hereafter we use only the *Louvain* method to detect communities.

2.1 Deactivation point and the generalized robustness

Even though there has been many works recently concerning the robustness of complex networks, there is not an unique definition of it [12–14, 16]. Robustness might be defined as the ability of a system to keep a set of defined features or services working when subject to perturbations or attacks [27]. This response to perturbations is tightly coupled to the goal of the real system subjacent to the graph representation in such a way that the robustness is service dependent [28].

Therefore, the robustness of complex abstract graphs, in which the system dynamics is not taken into account, should be addressed by either topological phase transition points or, in the absence of such behavior, by general functions representing the overall response of the network topology to a desired strategy of attack or fragmentation [29–34]. In this context, robustness is typically considered in a percolation framework and quantified by the critical fraction ρ_c of nodes that once removed by degree-based attacks leads to complete atomization of the network. At that point, one may safely say that the network stops functioning as whole because there is no giant component connecting the system according to the Molloy-Reed criterion. In this framework, in order to quantify the effect of the attacks on the networks [35], it is usually defined the order parameter $\sigma(\rho) = \frac{N_c}{N}$ as the relative size of the remainder network size relative to the original network size as a function of the fraction of nodes deleted.

However, modular networks usually present a transition point that marks a phase where all communities are detached from the main graph. At this point, the largest cluster size would be equal to the original network’s maximum module size N_{max} and the critical fraction of nodes that should be deleted in order to stop the normal operation of the network is given by what we call the deactivation point $P_d = (\sigma_d, \rho_d)$, where

$$\sigma_d = \frac{N_{max}}{N}, \quad (2)$$

is the size of the largest module as compared to the original network size and ρ_d is the fraction of independent interconnected nodes. This point depends on the modular structure of each network and after this phase is reached, communication would not be possible among large distant pieces of the network. In other words, this point marks a phase at which the network effectively stops functioning as a whole much earlier than the percolation threshold under hub attack and before the network atomizes completely.

On the other hand, in order to compare the deactivation threshold (ρ_d) of networks with different topologies, the size of the largest community (σ_d) would have to be similar for most network types. This is not the case as easily observed in Eq. 2. Besides, the attack set should be the same if we are interested in comparing different networks and multiple attack methods. Again, this is not case because module-based attacks usually generate attack lists much smaller than the network size. Therefore, we need a more general robustness approach to account for situations where the network loses its essential modular functionality before it collapses completely after a given number of nodes, much smaller than the original size of the network, is removed. In this sense, a more general approach considers the relative size of the largest remaining connected component of the network during the attack procedure.

Soares *et al.* have proposed an unique measure to quantify the robustness of a system facing malicious attacks [36], that resumes to the area of $\sigma(\rho)$ curve. Here, we generalize this concept for targeted attacks that end before all nodes are removed, such as the module-based attack. In this sense, the robustness of

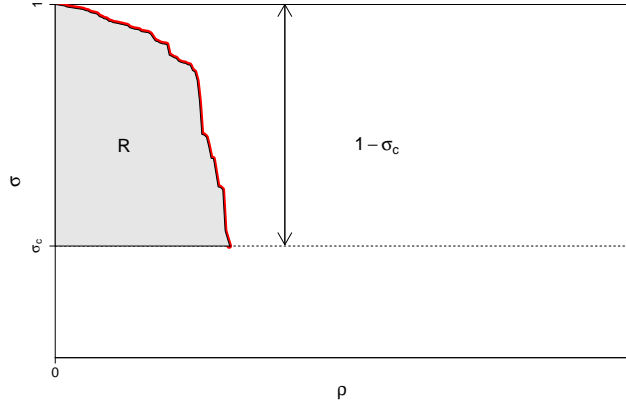


Figure 1: The figure depicts the geometric representation of the robustness as the ratio between the area underneath the red curve and the total area of possible attack given by area of the rectangle with sides lengths $1 - \sigma_c$ and 1 as defined in Eq. 3.

a network to a particular attack strategy is given by (see Fig. 1 for details):

$$R = \frac{1}{N(1 - \sigma_{min})} \sum_{\rho=0}^{\rho_{max}} \sigma(\rho) \quad (3)$$

where σ is the size of the largest connected component relative to the original size of the network, N is the number of nodes in the network, ρ is the fraction of nodes removed, ρ_{max} is the point at which the attack ends and σ_{min} is the value of the relative size of the largest connected component at ρ_{max} . This quantity measures the area underneath the σ curve relative to the maximum area of attack, *i.e.* the area of the rectangle delimited by the points $(0, \sigma_{min})$, $(0, 1)$, $(1, \sigma_{min})$, $(1, 1)$. In the MBA case, the point $(\rho_{max}, \sigma_{min})$ is the deactivation point (ρ_d, σ_d) .

2.2 Run-time and attack performance

Usually, the most used and efficient known methods of adaptive network attack are the high degree adaptive attack (HDA) and high betweenness adaptive attack (HBA). Therefore, from now on we compare the MBA procedure to these two methods. In order to study the connection between robustness and computation time we must calculate the time needed to perform each attack: HBA, HDA and MBA. Computing the betweenness centrality of all nodes in an unweighted network usually takes $\mathcal{O}(NE)$ time [37] while the degree complexity has a linear dependence $\mathcal{O}(N + E)$ [38]. On the other hand,

even though the exact computational complexity of the *Louvain* method is not known, it seems to run in time $\mathcal{O}(N \log N)$ [26]. Therefore, the computational run-time of MBA, HDA and HBA attacks are in increasing order of complexity $\mathcal{O}(NE + N \log N)$, $\mathcal{O}(\sum (\mathcal{N} + \mathcal{E}))$ and $\mathcal{O}(\sum \mathcal{N}\mathcal{E})$. As expected, MBA (even for dense graphs) is less expensive computationally than sequential methods, followed by HDA and HBA for a given network size.

In this sense, we may define the performance of an attack to a given network by:

$$\mathcal{P} = \frac{1}{t \times R} \quad (4)$$

where t is the time taken to complete the procedure in seconds and R is the robustness. In other words, \mathcal{P} measures the trade-off between the network robustness to a given attack and the time taken to complete the attack— a fast computing algorithm that efficiently fragments a network should result in high values of the attack performance \mathcal{P} , while very efficient attack methods that are in turn very slow should have attenuated performance values.

3 Results

We now generate multiple benchmark networks with varying size and modular structure according to Table 1. For both classes of undirected benchmarks (GN and LFR) the mixing parameter varies as $0.05 < \mu < 0.3$ and the modularity as $0.62 < Q < 0.93$. The next step is to analyze both the performance (\mathcal{P}) and the network robustness (R) according to each of the following fragmentation prescriptions: high degree adaptive attack (HDA), high betweenness adaptive attack (HBA) and module-based attack (MBA).

As can be seen in Fig. 2, networks with high modularity tend to be less robust to MBA attacks as expected. However, a new important feature of the MBA becomes clearer.

As the modularity of the networks is increased simultaneous MBA strongly outperforms adaptive degree attacks and more, for highly modular networks the robustness to MBA and high betweenness adaptive attack are very similar, with the MBA approach being much faster computationally than the sequential approach. This feature is easily seen by the network performance defined by Eq. 4. In Fig. 3 we plot \mathcal{P} with time measured as CPU time in seconds. Results show that the MBA approach has a better trade-off between efficiency and computational cost than adaptive methods. For the chosen LFR benchmarks the MBA performance always outperforms HBA and HDA performances, while for the GN benchmarks there is a critical modularity of approximately 0.7 from which $\mathcal{P}(MBA)$ is higher than in the adaptive approaches.

As a final case study, we address a real network representing the European power grid (EUPG) [39]. This system consists of 1494 nodes and 2322 edges and a node represents a generator, a transformer, or a substation, while edges represent a power supply line. The European power grid network is highly modular with a modularity extracted by the *Louvain* method of 0.89. As

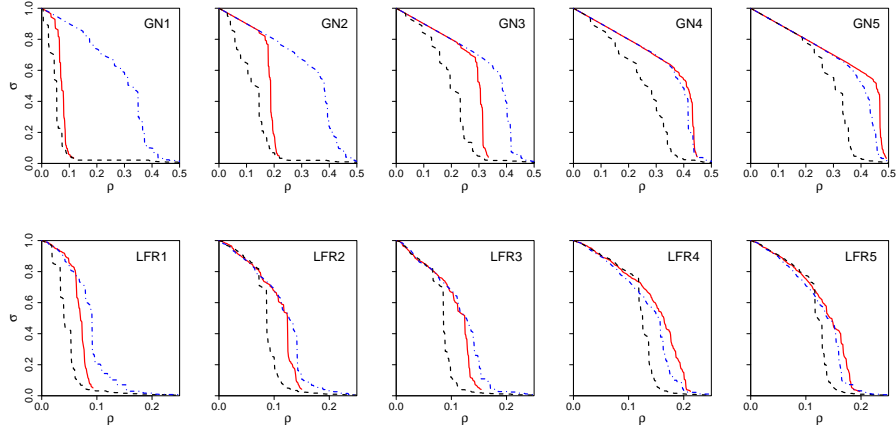


Figure 2: The fragmentation process presented by the relative size of the biggest component σ as a function of the fraction of removed nodes ρ following MBA, HBA and HDA attacks on the benchmark networks, Girvan-Newman (GN) and Lancichinetti-Fortunato-Raddichi (LFR) defined in Table 1. Modularity decreases from left to right. Solid red lines are MBA attacks, dashed black lines are HBA attacks and dashed-dotted lines are HDA attacks.

Net	N	E	μ	Q
GN1	1000	2500	0.05	0.93
GN2	1000	2500	0.10	0.87
GN3	1000	2500	0.15	0.81
GN4	1000	2500	0.20	0.76
GN5	1000	2500	0.30	0.62
LFR1	1000	2286	0.05	0.91
LFR2	1000	2385	0.10	0.86
LFR3	1000	2314	0.15	0.83
LFR4	1000	2392	0.20	0.76
LFR5	1000	2292	0.30	0.68
EUPG	1494	2322	-	0.89

Table 1: In this table we present the topological data for the five artificial networks of the Girvan-Newman class (GN1 - GN5), the five artificial networks of Lancichinetti-Fortunato-Radicchi class (LFR1 - LFR5) and the European power grid system (EUPG). The data consists of the network type, the number of vertices, the number of edges, the mixing parameter and the modularity.

shown in Fig. 3 and its inset, the performance of HDA, HBA and MBA attacks in the European power grid network are respectively $\mathcal{P}_{EUPG}(HDA) = 1.59$, $\mathcal{P}_{EUPG}(HBA) = 2.73$ and $\mathcal{P}_{EUPG}(MBA) = 15.65$. As expected by the analyzes on the benchmarks, in the power grid system the performance of the MBA prescription is much higher than performance HDA and HBA. Besides, the network is more fragile to non-adaptive MBA attack than to adaptive HDA attack and this is due to its highly modular nature.

4 General discussion and conclusion

In this contribution we have introduced a generalized robustness measure and an empirical performance quantity to measure the trade-off between computation time and robustness of modular networks facing general attack strategies. The two concepts were tested for a variety of well known homogeneous and heterogeneous benchmark networks which were attacked according to high degree adaptive attack, high betweenness adaptive attack and non-adaptive module-based attack. Computer simulations show that the module-based prescription perform better than degree and betweenness sequential attacks for highly modular networks —for instance, the European power grid the performance of the MBA is almost 10 times higher than the performance of HDA and almost 6 times higher than the performance of HBA. This outstanding result means that networks with well defined communities present robustness to MBA and HBA very similar but with less computational effort needed to atomize the network by the MBA procedure. Besides, the networks studied are more fragile to MBA than to traditional sequential hub attack. These outstanding features highlight

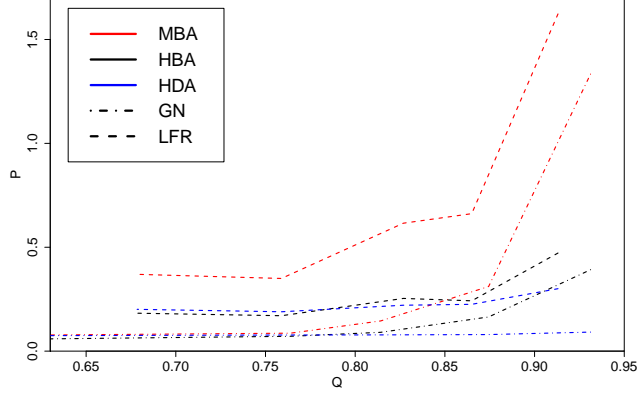


Figure 3: The figure shows the performance \mathcal{P} defined Eq. 4 as a function of the modularity Q for the ten networks detailed in Table 1. Red lines depict MBA attacks, blue lines HBA attacks and black lines HDA attacks. The benchmarks are divided with the dotted lines representing Girvan-Newman networks and the dashed lines the Lancichinetti-Fortunato-Radicchi benchmarks.

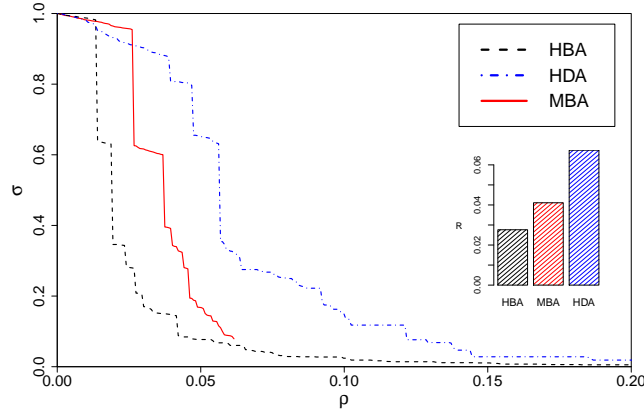


Figure 4: The figure shows the effect of attacking the European Union power grid with HDA, HBA and MBA strategies measured by the relative size of the largest connected component σ as a function of the fraction of removed nodes ρ . The inset displays the robustness of the network to all three attack strategies.

the importance of interconnected nodes in maintaining modular networks functioning as a whole. Likewise, we have introduced the concept of deactivation point where the network loses its functionality and modular structure, which generally happens much earlier than the percolation threshold usually used to quantify network robustness.

Finally, we have studied the performance \mathcal{P} , the deactivation point P_d , and the robustness for all three methods described above for a real network example: the European power grid. This network is highly modular and the attacks tried on it confirm that the non-adaptive MBA procedure performs better than both HDA and HBA. Therefore, in order for the power grid system be safer against malicious attacks, the modularity would decrease by, for instance, rewiring internal edges in order to increase the number of interconnected nodes.

The work is well posed as simulations were performed in a wide range of benchmark networks with varying topologies at which the MBA procedure is known to work very well. We believe that these results might have strong impacts in improving the robustness of real networks and/or in planning effective attack strategies to real systems.

5 Acknowledgments

SG acknowledges financial support from brazilian agency Conselho Nacional de Desenvolvimento Científico e Tecnológico through CNPq-MIT project #551974/2011-7. BRC acknowledges the brazilian Federal Police for financial support.

References

- [1] Mark Newman. *Networks: An Introduction*. Oxford University Press, May 2010.
- [2] Reuven Cohen and Shlomo Havlin. *Complex Networks: Structure, Robustness and Function*. Cambridge University Press, August 2010.
- [3] P. Holme. Efficient local strategies for vaccination and network attack. *EPL (Europhysics Letters)*, 68(6):908, 2004.
- [4] Lingyu Wang, Anoop Singhal, and Sushil Jajodia. Toward measuring network security using attack graphs. In *Proceedings of the 2007 ACM Workshop on Quality of Protection, QoP’07*, pages 49–54, New York, NY, USA, 2007. ACM.
- [5] Reuven Cohen, Keren Erez, Daniel ben Avraham, and Shlomo Havlin. Breakdown of the internet under intentional attack. *Physical Review Letters*, 86(16):3682–3685, Apr 2001.
- [6] Laurent Hébert-Dufresne, Antoine Allard, Jean-Gabriel Young, and Louis J. Dubé. Global efficiency of local immunization on complex networks. *Scientific Reports*, 3:2171 EP –, 07 2013.

- [7] Giuliano Andrea Pagani and Marco Aiello. The power grid as a complex network: A survey. *Physica A: Statistical Mechanics and its Applications*, 392(11):2688 – 2700, 2013.
- [8] M. Farhan Habib, Massimo Tornatore, and Biswanath Mukherjee. Cascading-failure-resilient interconnection for interdependent power grid - optical networks. In *Optical Fiber Communication Conference*, page M3I.3. Optical Society of America, 2015.
- [9] Paul AC Duijn, Victor Kashirin, and Peter MA Sloot. The relative ineffectiveness of criminal network disruption. *Scientific reports*, 4, 2014.
- [10] Jörg Raab and H Brinton Milward. Dark networks as problems. *Journal of public administration research and theory*, 13(4):413–439, 2003.
- [11] Réka Albert, István Albert, and Gary L. Nakarado. Structural vulnerability of the north american power grid. *Phys. Rev. E*, 69:025103, Feb 2004.
- [12] Paolo Crucitti, Vito Latora, Massimo Marchiori, and Andrea Rapisarda. Efficiency of scale-free networks: error and attack tolerance. *Physica A: Statistical Mechanics and its Applications*, 320:622–642, Mar 2003.
- [13] Réka Albert, Hawoong Jeong, and Albert-László Barabási. Error and attack tolerance of complex networks. *Nature*, 406(6794):378–382, Jul 2000.
- [14] Paolo Crucitti, Vito Latora, Massimo Marchiori, and Andrea Rapisarda. Error and attack tolerance of complex networks. *Physica A: Statistical Mechanics and its Applications*, 340(1-3):388–394, Sep 2004.
- [15] H. Jeong, S. P. Mason, A.-L. Barabási, and Z. N. Oltvai. Lethality and centrality in protein networks. *Nature*, 411(6833):41–42, May 2001.
- [16] Swami Iyer, Timothy Killingback, Bala Sundaram, and Zhen Wang. Attack robustness and centrality of complex networks. *PLoS ONE*, 8(4):e59613, 04 2013.
- [17] Petter Holme, Beom Jun Kim, Chang No Yoon, and Seung Kee Han. Attack vulnerability of complex networks. *Phys. Rev. E*, 65:056109, May 2002.
- [18] Sergey V. Buldyrev, Roni Parshani, Gerald Paul, H. Eugene Stanley, and Shlomo Havlin. Catastrophic cascade of failures in interdependent networks. *Nature*, 464(7291):1025–1028, Apr 2010.
- [19] M. E. J. Newman and M. Girvan. Finding and evaluating community structure in networks. *Phys. Rev. E*, 69:026113, Feb 2004.
- [20] Saray Shai, Dror Y Kenett, Yoed N Kenett, Miriam Faust, Simon Dobson, and Shlomo Havlin. Resilience of modular complex networks. *arXiv preprint arXiv:1404.4748*, 2014.

- [21] Louis M Shekhtman, Saray Shai, and Shlomo Havlin. Resilience of networks formed of interdependent modular networks. *New Journal of Physics*, 17(12):123007, 2015.
- [22] Bruno Requião da Cunha, Juan Carlos González-Avella, and Sebastián Gonçalves. Fast fragmentation of networks using module-based attacks. *PLoS ONE*, 10(11):e0142824, 11 2015.
- [23] M. Girvan and M. E. J. Newman. Community structure in social and biological networks. *Proceedings of the National Academy of Sciences*, 99(12):7821–7826, 2002.
- [24] Andrea Lancichinetti, Santo Fortunato, and Filippo Radicchi. Benchmark graphs for testing community detection algorithms. *Phys. Rev. E*, 78:046110, Oct 2008.
- [25] Andrea Lancichinetti and Santo Fortunato. Community detection algorithms: A comparative analysis. *Phys. Rev. E*, 80:056117, Nov 2009.
- [26] Vincent D Blondel, Jean-Loup Guillaume, Renaud Lambiotte, and Etienne Lefebvre. Fast unfolding of communities in large networks. *Journal of Statistical Mechanics: Theory and Experiment*, 2008(10):P10008, 2008.
- [27] Erica Jen. *Robust Design: A Repertoire of Biological, Ecological, and Engineering Case Studies. Studies in the Sciences of Complexity*. Oxford University Press, USA, 2005.
- [28] P Van Mieghem, C Doerr, H Wang, J Martin Hernandez, D Hutchison, M Karaliopoulos, and RE Kooij. A framework for computing topological network robustness. *Delft University of Technology, Report20101218*, 2010.
- [29] Tiago A. Schieber, Laura Carpi, Alejandro C. Frery, Osvaldo A. Rosso, Panos M. Pardalos, and Martín G. Ravetti. Information theory perspective on network robustness. *Physics Letters A*, 380(3):359 – 364, 2016.
- [30] Reuven Cohen, Keren Erez, Daniel ben Avraham, and Shlomo Havlin. Resilience of the internet to random breakdowns. *Physical Review Letters*, 85(21):4626–4628, Nov 2000.
- [31] Duncan S. Callaway, M. E. J. Newman, Steven H. Strogatz, and Duncan J. Watts. Network robustness and fragility: Percolation on random graphs. *Physical Review Letters*, 85(25):5468–5471, Dec 2000.
- [32] Cun-Lai Pu and Wei Cui. Vulnerability of complex networks under path-based attacks. *Physica A: Statistical Mechanics and its Applications*, 419(0):622 – 629, 2015.
- [33] Cun-Lai Pu, Wen-Jiang Pei, and Andrew Michaelson. Robustness analysis of network controllability. *Physica A: Statistical Mechanics and its Applications*, 391(18):4420–4425, Sep 2012.

- [34] Vladimir L. Boginski, Clayton W. Commander, and Timofey Turko. Polynomial-time identification of robust network flows under uncertain arc failures. *Optimization Letters*, 3(3):461–473, 2009.
- [35] Marc Barthélemy. Spatial networks. *Physics Reports*, 499(1):1–101, 2011.
- [36] C. M. Schneider, A. A. Moreira, J. S. Andrade, S. Havlin, and H. J. Herrmann. Mitigation of malicious attacks on networks. *Proceedings of the National Academy of Sciences*, 108(10):3838–3841, Feb 2011.
- [37] Ulrik Brandes. A faster algorithm for betweenness centrality*. *Journal of mathematical sociology*, 25(2):163–177, 2001.
- [38] Ulrik Brandes and Thomas Erlebach, editors. *Network Analysis, Methodological Foundations*, volume 3418. Springer Berlin Heidelberg, 2005.
- [39] Y. Shavitt and N. Zilberman. A structural approach for pop geo-location. *INFOCOM IEEE Conference on Computer Communications Workshops*, 2010, pages 1–6, 2010.